WHAT IS CLAIMED IS:

1. A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the twice-encrypted data to the intended image output device.

2. A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair,

a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

3. A method according to Claim 2, wherein the first key is randomly generated.

4. A method according to Claim 2, wherein the first encrypting step utilizes a symmetric encryption algorithm.

5. A method according to Claim 2, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

6. A method according to Claim 2, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

7. A method according to Claim 2, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

8. A method according to Claim 2, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

9. A method according to Claim 2, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains

information related to the identity of a person initiating the secure transmission.

10. A method according to Claim 9, further comprising:

a hashing step of processing the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and

a signing step of digitally signing the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

11. A method according to Claim 2, wherein the intended image output device is a printer.

12. A method according to Claim 2, wherein the intended image output device is a facsimile machine.

13. A method for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the method comprising:

a first encrypting step of encrypting the data using a first key;

a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being

primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

a generating step of generating a header containing the twice-encrypted first key;

a first transmitting step of transmitting the header to the intended image output device;

a receiving step of receiving a request from the intended image output device for the encrypted data; and

a second transmitting step of transmitting the encrypted data to the intended image output device.

14. A method according to Claim 13, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

15. A method according to Claim 13, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

16. A method for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving twice-encrypted data;

a decrypting step of twice decrypting the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating step of generating an image from the decrypted data.

17. A method for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving encrypted data and a twice-encrypted first key;

a first decrypting step of twice decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step of decrypting the encrypted data using the decrypted first key; and

an image generating step of generating an image from the decrypted data.

18. A method according to Claim 17, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

19. A method according to Claim 17, wherein the second decrypting step utilizes a symmetric decryption algorithm.

20. A method according to Claim 17, wherein the first decrypting step decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

21. A method according to Claim 17, wherein the first decrypting step decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key.

22. A method according to Claim 17, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

23. A method according to Claim 17, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

24. A method according to Claim 17, wherein the receiving step further receives a signed header hash and a signed data hash, the method further comprising a verifying step of verifying the

authenticity and the integrity of the signed header hash and of the signed data hash.

25. A method according to Claim 24, further comprising the step of discarding the encrypted data rather than outputting an image based upon the encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

26. A method according to Claim 25, further comprising the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

27. A method according to Claim 17, wherein the intended image output device is a printer.

28. A method according to Claim 17, wherein the intended image output device is a facsimile machine.

29. A method for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the method comprising:

a receiving step of receiving a header containing a twice-encrypted first key;

a sending step of sending a request for encrypted data corresponding to the header;

a receiving step of receiving encrypted data corresponding to the header;

a first decrypting step of twice decrypting the twice-encrypted first key using a second key and

a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step of decrypting the encrypted data using the decrypted first key; and

an image generating step of generating an image from the decrypted data.

30. A method according to Claim 29, wherein the header is received in the receiving step by e-mail.

31. A method according to Claim 29, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

32. An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device for receipt by an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) an encrypting step of twice encrypting the data using a first key and a second key, the first key being a public key of a first private

key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and (b) a transmitting step of transmitting the twice-encrypted data to the intended image output device.

33. An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) a first encrypting step of encrypting the data using a first key; (b) a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and (c) a transmitting step of transmitting the encrypted data and the twice-encrypted first key to the intended image output device.

34. An apparatus according to Claim 33, wherein the first key is randomly generated.

35. An apparatus according to Claim 33, wherein the first encrypting step utilizes a symmetric encryption algorithm.

36. An apparatus according to Claim 33, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

37. An apparatus according to Claim 33, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

38. An apparatus according to Claim 33, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

39. An apparatus according to Claim 33, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

40. An apparatus according to Claim 33, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

41. An apparatus according to Claim 40, wherein the executable process steps further comprise: (d) a hashing step of processing the header and the encrypted data with a hashing

algorithm, resulting in a header hash and a data hash; and (e) a signing step of digitally signing the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission, wherein the transmitting step further transmits the signed header hash and the signed data hash.

42. An apparatus according to Claim 33, wherein the apparatus is a computer and the intended image output device is a printer.

43. An apparatus according to Claim 33, wherein the apparatus is a computer and the intended image output device is a facsimile machine.

44. An apparatus according to Claim 33, wherein the apparatus is a first facsimile machine and the intended image output device is a second facsimile machine.

45. An apparatus for secure transmission of data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the apparatus comprising:

a memory including a region for storing executable process steps and data for the image; and

a processor for executing the executable process steps;

wherein the executable process steps include (a) a first encrypting step of encrypting the data using a first key; (b) a second encrypting step of twice encrypting the first key using a second key and a third key, the second key being a

public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; (c) a generating step of generating a header containing the twice-encrypted first key; (d) a first transmitting step of transmitting the header to the intended image output device; (e) a receiving step of receiving a request from the intended image output device for the encrypted data; and (f) a second transmitting step of transmitting the encrypted data to the intended image output device.

46. A method according to Claim 45, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

47. A method according to Claim 45, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

48. An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving twice-encrypted data;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a decrypting step of twice decrypting the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and (b) an image generating step of generating an image from the decrypted data.

49. An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving encrypted data and an twice-encrypted first key;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a first decrypting step of decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a

first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; (b) a second decrypting step of decrypting the encrypted data using the decrypted first key; and (c) an image generating step of generating an image from the decrypted data using the image generator.

50. An image output device according to Claim 49, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

51. An image output device according to Claim 49, wherein the second decrypting step utilizes a symmetric decryption algorithm.

52. An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the second key before decrypting the first key using the third key.

53. An image output device according to Claim 49, wherein the first decrypting step decrypts the first key using the third key before decrypting the first key using the second key.

54. An image output device according to Claim 49, wherein the third key is contained within the image output device, whereby the third key is primarily shielded from access by devices other than the image output device.

55. An image output device according to Claim 49, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

56. An image output device according to Claim 49, wherein the receiving step further receives a signed header hash and a signed data hash, the executable process steps further comprising a verifying step of verifying the authenticity and integrity of the signed header hash and of the signed data hash.

57. An image output device according to Claim 56, wherein the executable process steps further comprise the step of discarding the encrypted data rather than outputting an image, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

58. An image output device to Claim 57, wherein the executable process steps further comprise the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

59. An image output device according to Claim 49, wherein the image output device is a printer.

60. An image output device according to Claim 49, wherein the image output device is a facsimile machine.

61. An image output device for generating an image from data transmitted to the image output device, wherein the data can be used to generate the image at the image output device in the presence of an intended recipient, the image output device comprising:

a receiver for receiving a header containing a twice-encrypted first key;

an image generator for generating an image from image data;

a memory including a region for storing executable process steps and data; and

a processor for executing the executable process steps, wherein the executable process steps include: (a) a sending step of sending a request for encrypted data corresponding to the header; (b) a receiving step of receiving encrypted data corresponding to the header; (c) a first decrypting step of twice decrypting the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; (d) a second decrypting step of decrypting the encrypted data using the decrypted first key; and (e) an image generating step of generating an image from the decrypted data.

62. A method according to Claim 61, wherein the header is received by e-mail.

63. A method according to Claim 61, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

64. A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

an encrypting step to twice encrypt the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step to transmit the twice-encrypted data to the intended image output device.

65. A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

a first encrypting step to encrypt the data using a first key;

a second encrypting step to encrypt the first key twice using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

a transmitting step to transmit the encrypted data and the twice-encrypted first key to the intended image output device.

66. A computer-readable medium according to Claim 65, wherein the first key is randomly generated.

67. A computer-readable medium according to Claim 65, wherein the first encrypting step utilizes a symmetric encryption algorithm.

68. A computer-readable medium according to Claim 65, wherein the second encrypting step utilizes an asymmetric encryption algorithm.

69. A computer-readable medium according to Claim 65, wherein the second encrypting step encrypts the first key using the second key before encrypting the first key using the third key.

70. A computer-readable medium according to Claim 65, wherein the second encrypting step encrypts the first key using the third key before encrypting the first key using the second key.

71. A computer-readable medium according to Claim 65, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a device initiating the secure transmission.

72. A computer-readable medium according to Claim 65, wherein, in the transmitting step, the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

73. A computer-readable medium according to Claim 72, wherein the computer-executable process steps further comprise:

a hashing step to process the header and the encrypted data with a hashing algorithm, resulting in a header hash and a data hash; and

a signing step to digitally sign the header hash and the data hash with a private key of a third private key/public key pair, the private key of the third private key/public key pair being primarily maintained in the sole possession of the person initiating the secure transmission,

wherein the transmitting step further transmits the signed header hash and the signed data hash.

74. A computer-readable medium according to Claim 65, wherein the intended image output device is a printer.

75. A computer-readable medium according to Claim 65, wherein the intended image output device is a facsimile machine.

76. A computer-readable medium which stores computer-executable process steps which securely transmit data to an intended image output device, wherein the data can be used to generate an image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a data generating step to generate data for an image;

a first encrypting step to encrypt the data using a first key;

a second encrypting step to twice encrypt the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

a generating step to generate a header containing the twice-encrypted first key;

a first transmitting step to transmit the header to the intended image output device;

a receiving step to receive a request from the intended image output device for the encrypted data; and

a second transmitting step to transmit the encrypted data to the intended image output device.

77. A computer-readable medium according to Claim 76, wherein the first transmitting step transmits the header to the intended image output device by e-mail.

78. A computer-readable medium according to Claim 76, wherein the header which is generated in the generating step also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

79. A computer-readable medium which stores computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive twice-encrypted data;

a decrypting step to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating step to generate an image from the decrypted data.

80. A computer-readable medium which stores computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive encrypted data and a twice-encrypted first key;

a first decrypting step to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

a second decrypting step to decrypt the encrypted data using the decrypted first key; and

an image generating step to generate an image from the decrypted data.

81. A computer-readable medium according to Claim 80, wherein the first decrypting step utilizes an asymmetric decryption algorithm.

82. A computer-readable medium according to Claim 80, wherein the second decrypting step utilizes a symmetric decryption algorithm.

83. A computer-readable medium according to Claim 80, wherein the first decrypting step decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

84. A computer-readable medium according to Claim 80, wherein the first decrypting step decrypts the twice-encrypted first key using the third key before decrypting the twice-encrypted first key using the second key.

85. A computer-readable medium according to Claim 80, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

86. A computer-readable medium according to Claim 80, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

87. A computer-readable medium according to Claim 80, wherein the receiving step further receives a signed header hash and a signed data hash, the method further comprising a verifying step of verifying the authenticity and the integrity of the signed header hash and of the signed data hash.

88. A computer-readable medium according to Claim 87, further comprising the step of discarding the encrypted data rather than outputting an image based upon the encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

89. A computer-readable medium according to Claim 88, further comprising the step of sending a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

90. A computer-readable medium according to Claim 80, wherein the intended image output device is a printer.

91. A computer-readable medium according to Claim 80, wherein the intended image output device is a facsimile machine.

92. A computer-readable medium which stores computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

a receiving step to receive a header containing a twice-encrypted first key;

a sending step to send a request for encrypted data corresponding to the header;

a receiving step to receive encrypted data corresponding to the header;

a first decrypting step to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key

pair being primarily in the sole possession of the intended image output device;

a second decrypting step to decrypt the encrypted data using the decrypted first key; and

an image generating step to generate an image from the decrypted data.

93. A computer-readable medium according to Claim 92, wherein the header is received in the receiving step by e-mail.

94. A method according to Claim 92, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

95. A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

encrypting code for twice encrypting the data using a first key and a second key, the first key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the second key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

transmitting code for transmitting the twice-encrypted data to the intended image output device.

96. A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image; and

transmitting code for transmitting the encrypted data and the twice-encrypted first key to the intended printer.

97. A printer driver according to Claim 96, wherein the first key is randomly generated.

98. A printer driver according to Claim 96, wherein the first encrypting code utilizes a symmetric encryption algorithm.

99. A printer driver according to Claim 96, wherein the second encrypting code utilizes an asymmetric encryption algorithm.

100. A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the second key before encrypting the first key using the third key.

101. A printer driver according to Claim 96, wherein the second encrypting code encrypts the first key using the third key before encrypting the first key using the second key.

102. A printer driver according to Claim 96, wherein the twice-encrypted first key is contained in a header which also contains information related to the identity of a person initiating the secure transmission.

103. A printer driver according to Claim 102, wherein the header also contains a signed header hash and a signed data hash, and further comprising verification code for verification of the authenticity and integrity of the signed header hash and of the signed data hash.

104. A printer driver according to Claim 103, further comprising sending code for sending a notice to a sender of the header, if one of the signed header hash and signed data hash fails the verification of authenticity and integrity.

105. A printer driver which securely transmits data to an intended printer, wherein the data can be used to generate an image at the

intended printer in the presence of an intended recipient, the printer driver comprising:

data generating code for generating data for an image;

first encrypting code for encrypting the data using a first key;

second encrypting code for twice encrypting the first key using a second key and a third key, the second key being a public key of a first private key/public key pair, a private key of the first private key/public key pair being primarily in the sole possession of the intended image output device, and the third key being a public key of a second private key/public key pair, a private key of the second private key/public key pair being primarily in the sole possession of the intended recipient of the image;

generating code for generating a header containing the twice-encrypted first key;

first transmitting code for transmitting the header to the intended image output device;

receiving code for receiving a request from the intended image output device for the encrypted data; and

second transmitting code for transmitting the encrypted data to the intended image output device.

106. A printer driver according to Claim 105, wherein the first transmitting code transmits the header to the intended image output device by e-mail.

107. A printer driver according to Claim 105, wherein the header which is generated in the generating code also contains a reference to a location of the encrypted data, and wherein the

request for encrypted data contains the reference to the location of the encrypted data.

106. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive twice-encrypted data;

decrypting code to twice decrypt the twice-encrypted data using a first key and a second key, the first key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the second key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device; and

an image generating code to generate an image from the decrypted data.

107. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from twice-encrypted data transmitted to an intended image output device, wherein the twice-encrypted data can be used to generate the image at the intended image output device in the presence of an intended recipient, said computer-executable process steps comprising:

receiving code to receive encrypted data and a twice-encrypted first key;

first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

second decrypting code to decrypt the encrypted data using the decrypted first key; and

image generating code to generate an image from the decrypted data.

108. Computer-executable process steps according to Claim 107, wherein the first decrypting code utilizes an asymmetric decryption algorithm.

109. Computer-executable process steps according to Claim 107, wherein the second decrypting code utilizes a symmetric decryption algorithm.

110. Computer-executable process steps according to Claim 107, wherein the first decrypting code decrypts the twice-encrypted first key using the second key before decrypting the twice-encrypted first key using the third key.

111. Computer-executable process steps according to Claim 107, wherein the first decrypting code decrypts the twice-encrypted first key using

the third key before decrypting the twice-encrypted first key using the second key.

112. Computer-executable process steps according to Claim 107, wherein the third key is contained within the intended image output device, whereby the third key is primarily shielded from access by devices other than the intended image output device.

113. Computer-executable process steps according to Claim 107, wherein the second key is contained in a smart-card possessed by the intended recipient, whereby the second key is hidden from recipients other than the intended recipient.

114. Computer-executable process steps according to Claim 107, wherein the receiving code further receives a signed header hash and a signed data hash, the method further comprising verifying code to verify the authenticity and the integrity of the signed header hash and of the signed data hash.

115. Computer-executable process steps according to Claim 114, further comprising code to discard the encrypted data rather than outputting an image based upon the encrypted data, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

116. Computer-executable process steps according to Claim 115, further comprising code to send a notice to a sender of the signed header, if the signed header hash or the signed data hash fail the verification of authenticity and integrity.

117. Computer-executable process steps according to Claim 107, wherein the intended image output device is a printer.

118. Computer-executable process steps according to Claim 107, wherein the intended image output device is a facsimile machine.

119. Computer-executable process steps stored on a computer-readable medium, the computer-executable process steps for generating an image from data transmitted to an intended image output device, wherein the data can be used to generate the image at the intended image output device in the presence of an intended recipient, the computer-executable process steps comprising:

receiving code to receive a header containing a twice-encrypted first key;

sending code to send a request for encrypted data corresponding to the header;

receiving code to receive encrypted data corresponding to the header;

first decrypting code to twice decrypt the twice-encrypted first key using a second key and a third key, the second key being a private key of a first private key/public key pair, the private key of the first private key/public key pair being primarily in the sole possession of the intended recipient of the image, and the third key being a private key of a second private key/public key pair, the private key of the second private key/public key pair being primarily in the sole possession of the intended image output device;

second decrypting code to decrypt the encrypted data using the decrypted first key; and

image generating code to generate an image from the decrypted data.

120. Computer-executable process steps according to Claim 119, wherein the header is received by e-mail.

121. Computer-executable process steps according to Claim 119, wherein the header also contains a reference to a location of the encrypted data, and wherein the request for encrypted data contains the reference to the location of the encrypted data.

ADD A17